RSA Conference 2019
March 2019, San Francisco, USA
TeleTrusT presents "IT Security made in Germany"

Trust Seal
www.teletrust.de/itsmig

Moscone Center
North Expo
Stand No. 5671

Exhibiting TeleTrusT members

achelos
Avira
BDR
BMI/BSI
Cryptovision
Cryptshare
Detack
eco
Floragunn
Hornetsecurity
Infodas
IT Concepts
itWatch
Matrix42
MB Connect Line
MTG
NCP
QGroup
QuoScient
Secomba
Secunet
TÜViT

03.03.2019, 07:30 - 10:30pm - On invitation only
TeleTrusT Reception

——

04.03.2019, 10:30am - 04:20pm - Registration required
German-American Security Forum - Experience German-American Cyber Security Cooperation

- Part of Deutschlandjahr USA: "Wunderbar together" -

TeleTrusT - IT Security Association Germany in cooperation with BMI - German Federal Ministry of the Interior, Building and Community, BSI - German Office for Information Security, GACC - German American Chamber of Commerce and Symantec

Morrison & Foerster LLP
425 Market St
San Francisco
CA 94105

Moderation: Prof. Dr. Norbert Pohlmann, Chairman of TeleTrusT

10:30 - 10:45am Greetings
Hans-Ulrich Suedbeck, German Consul General; Kristian Wolf, German American Chamber of Commerce, Managing Director

10:45 - 11:45am VIP Keynotes

1. Andreas Koenen, Federal Ministry of the Interior, Building and Community, Director General CI, Cyber- and Information Security
Cyber security of critical infrastructures - current developments in Germany and Europe
2. Jeff Greene, Symantec, Vice President, Global Government Affairs & Policy
Cyber security: a global responsibility
3. Dr. Rainer Baumgart, secunet, CEO
"Where do we come from and where are we going? A short story about Quantum Computing"
4. Dr. Allan Friedman, US Department of commerce, NTIA, Director of Cybersecurity Initiatives
"Resilience in a vulnerable world: policy and practice“

11:45am - 12:45pm Lunch

12:45 - 03:20pm Security Solutions Showcase

Cyberattacks aiming at fraud, espionage and sabotage are among the most serious threats our economies are facing today. In the light of the EU Data Protection Regulation coming into effect, this dialog presents European strategies and newest innovations for the security of the IoT. In particular, the effect of attacks on cross-linked devices and the defense of new attack technologies are discussed. We invite you to recognize cooperation possibilities with excellent providers of German IT security solutions.

Moderation: Thomas Hemker, Symantec

1. Stefan Mueller, Technical Expert, MB connect line
The evolution of the automation firewall

With the emergence of IoT, the automation firewall mbSEBRIN addresses the three main challenges between IT and OT: usability, miniaturization and security for legacy systems. This pocket-sized, self-learning firewall takes up the least amount of space possible in the control cabinet, can be easily installed, even by non-professionals, and is specifically designed for the automation user´s workflow.

2. Dr. Matthias Pankert, Senior Vice President, Utimaco IS (Germany)
Hung Troung, Vice President of Engineering, Utimaco Inc. (USA)
Building a German-US leader in hardware security - Utimaco acquires US competitor Atalla

Utimaco was founded in 1964 in Germany and has been in the IT security business since 1983. Utimaco is one of leading manufacturers of hardware security modules. Atalla was founded in 1973 in Silicon Valley, becoming a pioneer of hardware security modules. While Utimaco has been able to capture a significant market presence in Europe and in the segment of general purpose HSMs, its market position in America and in the electronic payment market has not been competitive in the last years.
The acquisition of the Atalla business by Utimaco has been a perfect match for both of our businesses. We have been able to complement each other with our respective strengths, with nearly no overlaps. In our presentation, we will address both the acquisition process and the integration of the two units which will fuel tremendous growth for our combined business, along with a number of key learnings that we have been able to make during our first few months together.

3. Heinfried Cznottka, Director Business Development, achelos
Security aspects in IoT connectivity
How to architect and validate security aspects for IoT devices connected via mobile networks

More and more (I)IoT devices are manufactured with embedded SIMs/UICCs (eSIM/eUICC) in order to have a scaling effect during production. A challenge is the provisioning of these devices in a secure way while maintaining security in the whole process. One way of implementing this is the remote provisioning of the physical SIMs or eSIMS rather than swapping them or even swapping the device. The GSMA Remote SIM provision opens a standardized way to provide such IoT devices with an operator specific profile after commissioning the device. This speech gives an overview of the security architecture, the security mechanisms

and the challenges faced to guarantee the end-to-end security of the environment from the IoT device to the remote provisioning software. We will give an example of a vendor independent implementation requiring a more comprehensive security management.

4. Matthias Kess, CTO, Befine Solutions
Making email wunderbar - security, audit trail and unlimited attachment size for your existing email system

Email is the most widely used electronic communication method of our time. Users love email and email is here to stay. However, shortcomings in terms of security, traceability and size limitations often force us to go other ways which sometimes violate compliance and are too complex for users to work with. Learn how Cryptshare can enable your existing email system to meet business requirements and make it the central medium for secure communication and file transfer. Making email wunderbar - security, audit trail and unlimited attachment size for your existing email system.

5. Richard O. Jorolemon, Office of the CISO, Lead Manager Infrastructure Security, AXA Equitable
John Waters, Director Business Developmet, Detack
Password analytics & quality assurance with EPAS: AXA Equitable (North America)

Rick Jorolemon will share AXA's experience in implementing password quality assurance with EPAS over the past five years, as well as the remediation measures taken to reach a regulated compliant and high security environment while still relying on classic password authentication. Supported by John Waters of Detack, he will briefly present the controls and enforcement measures provided by EPAS that AXA has been using over the past years in the USA.

6. Dr. Bruno Quint, Director Cloud Encryption, Rohde & Schwarz Cybersecurity
No more an oxymoron: customer-side encrypted collaborative cloud-based applications

Trusted Gate provides a high security enablement for existing business applications like MS Office 365. Customers will be able to run their business transparently in public cloud systems but keep their original data on configurable storage systems. Trusted Gate also provides a meta-cloud layer which enables business applications to use and interact with security solutions and storage systems across different clouds, completely transparent and with highest data centric security. Supported cloud platforms are AZURE, AWS and Google.

7. Juergen Ruf, Chairman of the Board, MTG
Real world post-quantum cryptographic security solutions

The presentation will briefly present these new post-quantum cryptography algorithms and focus on the challenges of integrating them into an existing security infrastructure. Especially, the necessary steps for the transition from traditional to post-quantum algorithms and the possibilities of combining them will be addressed. Furthermore, real world applications that take advantage of PQC algorithms will be showcased.

)* Presentations in collaboration with US companies

03:20 - 04:20pm VIP Panel

Moderation: Dr. Alexander Schellong, INFODAS

Strategic expert discussion on current IT security trends

a. The policy challenge for government agencies to report vulnerabilities or keep them secret for national security purpose
b. IoT / other product IT Security certifications and holding device makers accountable for breaches caused by devices

Panel
- Andreas Koenen, Federal Ministry of the Interior, Building and Community, Director General CI, Cyber- and Information Security
- Dr. Udo Helmbrecht, ENISA - EU Cybersecurity Agency, President
- Dr. Allan Friedman, US Department of Commerce, NTIA, Director of Cybersecurity Initiatives

04.03.2019, 05:00pm
German Pavilion Opening

———

05.03.2019, 04:00 - 06:00pm
Wine Event - RSA German Pavilion

———

06.03.2019, 09:00 - 11:00am - Registration required
TeleTrusT/FIDO Alliance: German/US Expert Meeting

AMA - San Francisco Executive Conference Center
R 213/214
55 4th St
San Francisco
CA 94103

Join the event to meet industry experts and hear about the latest trends in strong authentication. Attendees will get insights from companies that have led real-world FIDO deployments, an inside view on how FIDO authentication provides solutions to the regulatory challenges posed by PSD2, eIDAS and GDPR as well as discussions on related initiatives and technologies in the US and in Germany.

Agenda highlights:

- Key updates from FIDO Alliance
- Deployment case studies: Hands-on insights from organizations that have deployed FIDO (with a particular focus on FIDO solutions aligned to the requirements of European regulations like eIDAS)
- Latest updates of FIDO authentication in Germany (for example in automotive industry)
- Open discussion

Moderation: Malte Kahrs, MTRIX

Panel
- Prof. Dr. Norbert Pohlmann, TeleTrusT
- Dr. Kim Nguyen, Bundesdruckerei
- Udo Helmbrecht, ENISA
- Joachim Weber, BSI
- Joerg Borchert, Infineon
- Brett McDowell, FIDO Alliance
- Dirk Balfanz, Google
- Sam Shrinivas, Google
- Anthony Nadalin, Microsoft
- John Fontana, Yubico/FIDO EWG
- Adam Ross, Cryptovision
- Sami Nassar, NXP

———

06.03.2019, 01:30 - 02:20pm
TeleTrusT Session (RSA Gold Sponsor Slot): "Innovative Answers to IoT Security Challenges"

Moscone South Esplanade 154

Julian Weinberger, NCP engineering GmbH, Director of Systems Engineering: "Industry 4.0 provides a new revolutionary approach in automation and data exchange in manufacturing. The new technology does not only create new opportunities but also multiple challenges for IT departments, operations and vendors. The threat landscape increases dramatically through more connected devices. Industry 4.0 involves different parties with different challenges. Security is hereby one challenge all parties have in common and together a solution can be found."

Moderation: Prof. Norbert Pohlmann, TeleTrusT

Panel
- Jean-Paul Verheylewegen, MB Connect Line, Global Sales Manager
- Heinfried Cznottka, achelos, Director Business Development
- Dr. Kim Nguyen, D-Trust, Managing Director

Industry 4.0 is all about seamless connectivity, convenient web services, and data exchange across the factory floor. With an increase in connected devices, OT cybersecurity is essential. Today, OT is mostly unprepared and hackers, once beyond IT security, find an open field and vulnerable devices to exploit. OT cybersecurity complements IT efforts and enhances the overall cybersecurity. The growing deployment of new generations of (I)IoT devices and the integration into factory and office networks creates new challenges to ensure communication security. In the panel session we discuss innovative ways for identity management, securely enabling connectivity of IoT devices and enabling security for legacy systems while keeping the usability at a high level. PKI has been one of the most foremost methods to make trusted identities available in the digital world, this applies to personal identities (e.g. in authentication) but also to organizational and technical entities (e.g. in server certificates). PKI is a centralized and trusted technology in organizations and institutions. In the past two years Blockchain or more generally speaking distributed ledger technologies have gained considerable attention and the claim exists that these technologies will revolutionize identity management and substitute PKI in general. We argue that this is not the case, showing how Blockchain technologies can be used in order to enhance trust in PKI systems in various ways. Examples will be provided ranging from application scenarios of server certificates, mail encryption and IoT.

———

06.03.2019, 07:00 - 10:00pm - On invitation only
Reception at German Consulate General

IT Security Association Germany (TeleTrusT)
TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the quality seal "IT Security made in Germany" and runs the IT expert certification programs "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany